UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/065,291	10/01/2002	Xiao-Qin Yu	IACP0019USA	5715

27765 7590 09/15/2006

NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION
P.O. BOX 506
MERRIFIELD, VA 22116

EXAMINER	
TO, BAOTRAN N	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/065,291	YU ET AL.	
	Examiner	Art Unit	
	Baotran N. To	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action responds to the Applicant's Amendment filed on 07/07/2006.

Claims 1, 3 and 14 are amended.

Claims 1-14 are pending in the application.

Response to Arguments

2. Applicant's arguments filed 07/07/2006 have been fully considered but they are not persuasive.

Applicant argues, "However, Shambroom does not teach that the key distribution center 400 then sends the session key to the client 200. Instead, the key distribution center sends the key to a Kerberos Initialization Client 780 instead of the client 600. Therefore, Shambroom does not teach the limitation in claim 1 of 'controlling the access point to transmit the pair of crypto-keys to the first client'."

Examiner respectfully disagrees with this argument. Shambroom clearly discloses "KDC 400 then sends both the encrypted session key and the permission indicator back to the network server 300 as indicated at arrow 354. Network server 300 receives the encrypted information from KDC 400, and decrypts the KDC session key using client 200's user key. Both the permission indicator and the KDC session key are stored in credentials cache 320. Web server 305 encodes the contents of the credentials cache 320 and, as indicated at arrow 37, sends the content of the credentials cache 320 to the web browser 205" (Figure 3, col. 8, lines 38-50).

Applicant further argues, "In addition, regarding claims 6 and 9, Shambroom also does not teach 'transmitting the second key from the first user client through the access point to the second user client.' Instead, Shambroom only discloses that the client 200 sends a command to the destination server 500 through the network server 300. The destination server 500 is not a client. Thus, Shamhroom does not teach a second client, or sending a key from a first client to a second client through the access point."

Examiner respectfully disagrees with this contention. Shambroom specifically discloses, "Sending a command to a destination server. Now that it has the encoded credentials cache information from cache 320, client 200 can send this cache information along with a message, such as a command ultimately intend for destination server 500, to the network server 300 as indicated at arrow 358" (col. 8, line 66 – col. 9, line 2). Shambroom further discloses, " Thereafter, network server 300 decrypts the copy of the server session key that is encrypted using the KDC session key. Network server 300 then encrypts the message or command, using the server session key and, as indicated at arrow 64, sends the encrypted message along with the access indicator and a new authenticator to destination server 500 via secure network 450. Destination server 500 uses its own private key to decrypt and obtain the server session key" (col. 9, lines 37-41). Destination server can be a second client according to the claim limitations.

For at least above reasons, it is believed that the rejection is maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom (U.S. Patent 6,198,824 B1) hereinafter Shambroom in view of Eschelbeck et al. (U.S. Patent 6,611,869 B1) hereinafter Eschelbeck.

Regarding Claim 1, Shambroom discloses a method for applying for crypto-keys from a network system, the network system comprising at least a first user client, an access point having an identifying module and a user list, and a certificate server, the access point being used to receive a certificate packet from the first user client and to utilize the identifying module to verify the certificate packet according to the user list so as to generate a verification signal, the certificate server being used to generate a pair of distinct crypto-keys according to the verification signal and a first algorithm (see Figure 4), the method comprising:

utilizing the first user client (client 200) to generate the certificate packet (col. 7, lines 40-55);

utilizing the access point (network server 300) to receive the certificate packet (col. 7, lines 45-50);

utilizing the identifying module to verify the certificate packet according to the user list so as to generate the verification signal (col. 2, lines 30-35 and col. 8, lines 16-23), and

transmitting the verification signal to the certificate server (col. 8, lines 15-20);

controlling the certificate server to transmit the pair of crypto-keys to the access point (Figure 5-5A, col. 8, lines 37-50 and col. 9, lines 28-32); and

controlling the access point to transmit the pair of crypto-keys to the first client (col. 8, lines 37-50 and col. 10, line 55 through col. 11, lines 1-10).

Shambroom does not explicitly disclose "utilizing the certificate server to generate the pair of distinct crypto-keys according to the first algorithm."

However, Eschelbeck expressly discloses utilizing the certificate server to generate the pair of distinct crypto-keys according to the first algorithm (col. 6, lines 30-35).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Eschelbeck's invention with Shambroom to provide utilizing the certificate server to generate the pair of distinct crypto-keys according to the first algorithm. One of ordinary skill in the art would have been motivated to allow for enhancing the security of a message sent through a network (Abstract of Shambroom).

Regarding Claim 2, Shambroom and Eschelbeck disclose the limitations of Claim 1 above. Furthermore, Shambroom discloses wherein the certificate packet comprises a user name and a password (col. 8, lines 15-20).

Regarding Claim 3, Shambroom and Eschelbeck disclose the limitations of Claim 1 above. Furthermore, Eschelbeck discloses wherein the first algorithm is a Rivest Shamir Asleman (RSA) algorithm (col. 2 lines 35-40).

Regarding Claim 4, Shambroom and Eschelbeck disclose the limitations of Claim 1 above. Furthermore, Eschelbeck discloses wherein the first algorithm is a digital signature algorithm (DSA) (col. 5, lines 50-65).

Regarding Claim 5, Shambroom and Eschelbeck disclose the limitations of Claim 1 above. Furthermore, Eschelbeck discloses wherein the pair of crypto-keys is a public key and a private key (col. 6, lines 30-35).

Regarding Claim 6, Shambroom and Eschelbeck disclose the limitations of Claim 1 above. Furthermore, Shambroom discloses wherein the network system further comprises at least a second user client communicating with the access point, and the first user client comprises a first encryption module for encrypting a plain text into a ciphered text according to a second algorithm and a first key of the pair of crypto-keys, the second user client comprises a second decryption module for decrypting the

ciphered text into the plain text according to a third algorithm and a second key of the pair of crypto-keys (Figure 3), the method further comprising:

transmitting the second key from the first user client through the access point to the second user client (destination server) (Figure 1, (col. 8, line 66 – col. 9, line 2 and 9, lines 37-41);

utilizing the first encryption module to encrypt the plain text into the cipher text according to the second algorithm and the first key (col. 7, lines 30-35);

transmitting the ciphered text from the first user client through the access point to the second user client (col. 7, lines 40-45); and

utilizing the second decryption module to decrypt the ciphered text according to the third algorithm and the second key (col. 7, lines 40-45).

Regarding Claim 7, Shambroom and Eschelbeck disclose the limitations of Claim 6 above. Furthermore, Eschelbeck discloses wherein the second algorithm and third algorithm are associated with the first algorithm (col. 2, lines 35-40).

Regarding Claim 8, Shambroom and Eschelbeck disclose the limitations of Claim 6 above. Furthermore, Shambroom discloses wherein the first user client further-comprises a first decryption module for decrypting the ciphered text into the plain text according to the third algorithm and the first key, and the second user client further comprises a second encryption module for encrypting the plain text into the ciphered

text according to the second algorithm and the second key (Figure 3), the method further comprising:

utilizing the second encryption module to encrypt the plain text into the ciphered text according to the second algorithm and the second key (col. 9, lines 10-30);

transmitting the from the second user client through the access point to the first user client (col. 9, lines 10-15); and

utilizing the first decryption module to decrypt the ciphered text according to the third algorithm and the first key (col. 9, lines 40-50).

4. Claims 9-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom and Eschelbeck as applied to claim 1 above, and further in view of Sandhu et al. (U.S. Patent 7,017,041 B2) hereinafter Sandhu.

Regarding Claim 9, Shambroom and Eschelbeck disclose the limitations of Claim 6 above. Furthermore, Shambroom discloses wherein the network system further comprises at least a second user client communicating with the access point, and the first user client comprises a first encryption module for encrypting numbers according to a second algorithm and a first key of the pair of crypto-keys, the second user client comprises a second decryption module for decrypting numbers according to a third algorithm and a second key of the pair of crypto-keys (Figure 3 and , the method further comprising:

transmitting the second key from the first user client through the access point to the second user client (Figure 1, (col. 8, line 66 – col. 9, line 2 and 9, lines 37-41);

controlling the first user client to convert a plain text into a first value according to a fourth algorithm (col. 7, lines 25-50);

utilizing the first encryption module to encrypt the first value according to the second algorithm and the first key (col. 8, lines 15-35);

transmitting the and the encrypted first value from the first user client through the access point to the second user client (col. 10, lines 35-50);

utilizing the second decryption module to decrypt the encrypted first value according to the third algorithm and the second key (col. 9, lines 30-40);

Shambroom and Eschelbeck do not disclose "controlling the second user client to convert the plain text into a second value according to the fourth algorithm; and comparing the second value with the decrypted first value to verify the plain text transmitted from the first user client to the second user client."

However, Sandhu expressly discloses controlling the second user client to convert the plain text into a second value according to the fourth algorithm; and comparing the second value with the decrypted first value to verify the plain text transmitted from the first user client to the second user client (col. 1, lines 50-67 through col. 2, lines 1-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have combined Shambroom's invention and Eschelbeck's invention with Sandhu to include controlling the second user client to

convert the plain text into a second value according to the fourth algorithm; and comparing the second value with the decrypted first value to verify the plain text transmitted from the first user client to the second user client. One of ordinary skill in the art would have been motivated to allow for enhancing the security of a message sent through a network (Abstract of Shambroom).

Regarding Claim 10, Shambroom, Eschelbeck and Sandhu disclose the limitations of Claim 9 above. Furthermore, Sandhu discloses wherein the fourth algorithm is a message digest 2 (MD2) algorithm (col. 2, lines 15-25).

Regarding Claim 11, Shambroom, Eschelbeck and Sandhu disclose the limitations of Claim 9 above. Furthermore, Sandhu discloses wherein the fourth algorithm is a message digest 5 (MD5) algorithm (col. 2, lines 15-25).

Regarding Claim 12, Shambroom, Eschelbeck and Sandhu disclose the limitations of Claim 9 above. Furthermore, Sandhu discloses wherein the fourth algorithm is a secure Hash algorithm (SHA) (col. 2, lines 15-25).

Regarding Claim 13, Shambroom, Eschelbeck and Sandhu disclose the limitations of Claim 9 above. Furthermore, Sandhu discloses wherein the second algorithm and third algorithm are associated with the first algorithm (col. 3, lines 15-25).

Regarding Claim 14, Shambroom, Eschelbeck and Sandhu disclose the limitations of Claim 9 above. Furthermore, Sandhu discloses wherein the first user client further comprises a first decryption module for decrypting numbers according to the third algorithm and the first key, and the second user client further comprises a second encryption module for encrypting numbers according to the second algorithm and the second key (Figure 4), the method further comprising:

controlling the second user client to convert the plain text to the first value according to the fourth algorithm (col. 20, lines 15-45);

utilizing the second encryption module to encrypt the first value according to the second algorithm and the second key (col. 8, lines 45-65);

transmitting the and the encrypted first value from the second user client through the access point to the first user client (col. 7, lines 20-45);

utilizing the first decryption module to decrypt the encrypted first value according to the third algorithm and the first key (col. 6, lines 15-25);

controlling the first user client to convert the plain text to the second value according to the fourth algorithm (col. 1, lines 50-67 through col. 2, lines 1-25); and

comparing the second value with the decrypted first value to verify the plain text transmitted from the second user client to the first user client (col. 2, lines 1-25).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BTT
09/08/2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100